



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 24 December 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports that a cow in Washington state has tested presumptively positive for mad cow disease. (See item [15](#))
- CNET News.com reports Apple Computer has issued a security update that, among other fixes, closes a hole in Mac OS X that could have allowed hackers to take control of a computer under particular circumstances. (See item [26](#))
- eSecurity Planet reports anti-virus vendors on December 22, issued upgraded threat warnings for a mutant of the W32/Sober-C worm now squirming its way through e-mail in-boxes. (See item [28](#))

DHS/IAIP Update Fast Jump

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: HIGH, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. **December 23, Reuters** — California quake shuts power plant, triggers outages. The California power grid operator said a 700 megawatt, four-unit power plant was knocked out of service by the strong earthquake that struck the Central California coast on Monday, December 22. Lorie O'Donley, spokesperson for the California Independent System Operator, declined to name which plant was shut but confirmed it was not the giant Diablo Canyon nuclear power plant in Avila Beach, which continued to run. "There have been limited

outages in PG&E and (Southern California) Edison territories. I don't have any details," she said, adding that **there were no reports of damage from the earthquake to the region's high-voltage transmission lines.**

Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2003_12_22_eng-reuters_pma_CALIF-QUAKE-SHUTS-POWER-PLANT-TRIGGERS-OUTAGES&SMContentSet=0

2. *December 23, North American Electric Reliability Council* — **NERC issues 2003–2012 reliability assessment.** The North American Electric Reliability Council (NERC) issued its 2003 –2012 Reliability Assessment on Tuesday, December 23. "Generating resources are expected to be adequate throughout North America in the near term," stated Michehl R. Gent, NERC president and CEO. **Transmission systems in North America are expected to perform reliably in the near term, although the report notes that in some areas these systems are reaching their reliability limits. Previously seen transmission constraints are recurring, while new constraints are appearing as electricity flow patterns change, the report states.** The assessment points out that transmission expansion is not keeping up with expansion of generation and growth of demand, and notes that some portions of the grid will not be able to transmit the output of all new generating units to their targeted markets. Electricity demand is expected to grow by about 67,000 MW during the next five years, and resource additions over this period are projected to total about 89,000 MW, depending upon the number of new plants assumed to be in service. Report:
ftp://www.nerc.com/pub/sys/all_updl/docs/pubs/2003RAS.pdf
Source: ftp://www.nerc.com/pub/sys/all_updl/docs/pressrel/12-23-03-RAS-PR.pdf
3. *December 23, The Hampton Union (NH)* — **Plant responds to increase in threat level.** Seabrook nuclear plant, located near Portsmouth, NH, has stepped up security procedures in response to the heightened national threat level, according to nuclear power plant spokesperson David Barr. Specific safety measures cannot be discussed, Barr said, but added that the one visible change the station has undergone is to not allow visitors to tour the station until the threat is lowered. The U. S. government raised the national threat level to orange Sunday, saying that terrorist strikes were a possibility over the holidays. Barr also said the station receives word when any flights are scheduled to fly over the station. "If there is going to be an aircraft in the area, there's always advanced notice," Barr said. "Our security force is in constant contact with law enforcement, on the state, local and federal level."
Source: http://www.seacoastonline.com/news/hampton/12232003/news/670_62.htm

[\[Return to top\]](#)

Chemical Sector

4. *December 23, Bowling Green Kentucky KY Daily News* — **County has 17 sites with very hazardous, chemicals; teams train for emergencies.** Seventeen locations in Bowling Green and Warren County, KY, contain a total of nine very hazardous chemicals, as substances are designated by the federal government, according to Bob Myatt, chairman of Bowling Green/Warren County Emergency Planning Committee. The emergency planning committee maintains a list of those locations and chemicals, as required by the 1986 Superfund Amendments and Reauthorization Act. **About 5,000 chemicals are identified as hazardous**

— whether flammable, carcinogenic or simply poisonous — according to Ronnie Pearson, director of Warren County Emergency Management. Only about 60 of those are found in Warren County, and of those, only nine are classed as very dangerous. The materials are distributed among factories, pipelines and government facilities, Pearson said. The three most common very dangerous substances, according to Myatt, are chlorine (of which Bowling Green Municipal Utilities keeps up to 14,000 pounds), anhydrous ammonia and sulfuric acid. The majority of the chemicals, however, are much less dangerous — things like gasoline, diesel fuel and paint thinner. Operations that use extremely dangerous substances have their own fully equipped emergency response teams, he said.

Source: http://www.bgdailynews.com/cgi-bin/view.cgi?/200312/23+chemical20031223_news.html+20031223+news

[[Return to top](#)]

Defense Industrial Base Sector

5. *December 23, Government Computer News* — **Air Force sets to work on combat intranet upgrade.** The Air Force plans to redesign major components of its Combat Information Transport System intranet. The service has awarded a private contractor a nine-month, \$5 million contract to reconfigure both the unclassified and classified operations of the network by creating a common infrastructure. The project will also include an upgrade of the intranet's information assurance program. **The redesign will improve the Air Force's network security and consolidate staffs that now manage combat network operations and information assurance at the service's network operations and security centers,** the contractor said in a statement.

Source: http://www.gcn.com/vol1_no1/daily-updates/24494-1.html

[[Return to top](#)]

Banking and Finance Sector

6. *December 23, Buffalo Business First (NY)* — **Warning issued on counterfeit Canada Post orders. The New York State Banking Department has issued an alert to banks and the public that counterfeit Canada Post money orders are being sent to U.S. citizens for payment on services or products bought over the Internet.** The fraudulent money orders are for amounts much larger than \$999.99, the maximum value of legitimate Canada Post money orders. Bethany Blankley, a banking department public affairs officer, said the warning originated with Canadian authorities and the U.S. Treasury Department. As part of the scam, the U.S. victims are instructed to cash the money orders and send or deliver all or part of the proceeds to the scam artists. The computer-generated fake money orders do not contain the beaver watermark found on the top half of authentic ones and also contain fraudulent telephone numbers printed on the backside for verification purposes.

Source: http://buffalo.bizjournals.com/buffalo/stories/2003/12/22/daily11.html?jst=b_in_hl

7.

December 22, Associated Press — **U.S. freezes funds of three linked to al Qaeda.** The Bush administration acted Monday, December 22, to financially paralyze two foreign entities and an individual believed to be providing money for al Qaeda's terror network. **The Department of Treasury added to its list of suspected terrorist financiers: Vazir, a nonprofit organization headquartered in Travnik, Bosnia; a key representative of the group, Safet Durguti; and Hochburg AG, a company located in Vaduz, Liechtenstein. The department's designation freezes any of the three's financial assets in this country.** It also means they are prohibited from conducting financial transactions in the United States and bars Americans from doing business with them. The United States and Saudi Arabia also asked the United Nations to add the three names to its blocking list, which is honored by member countries, the Department of Treasury said.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A22630-2003Dec 22.html>

[[Return to top](#)]

Transportation Sector

8. *December 23, USA TODAY* — **Hijacked foreign jet among fears.** "There are concerns about a possible hijacking overseas at one of the locations where we think the security may not be at levels that inspire confidence," said Brian Jenkins, a counterterrorism expert and special adviser to the Rand Corp., a think tank. "Commercial aviation is very much in the al Qaeda playbook." **Security analysts in the U.S. have long worked with governments in Latin America, the Caribbean and developing nations in Africa and the Middle East to try to improve aviation security. But airline security remains lax in many of those nations' aviation systems, often because of a lack of money to pay for costly security programs. Even the European Union, which had agreed to improve the screening of checked baggage at airports by the end of 2002, has pushed back that deadline because of the costs of improved screening.** Such security shortcomings in other countries — over which the United States has little influence — are particularly worrisome, officials say.

Source: <http://www.usatoday.com/news/washington/2003-12-22-terror-al ert x.htm>

9. *December 23, Associated Press* — **Airports to fingerprint international visitors.** Foreigners entering U.S. airports and seaports — except those from Western Europe and a handful of other countries — will soon have their fingerprints scanned and their photographs snapped as part of a new program designed to enhance border security. **The program, to be up and running on January 5, at all 115 airports that handle international flights and 14 major seaports, will let Customs officials instantly check an immigrant or visitor's criminal background. The program, called US-VISIT, or U.S. Visitor and Immigrant Status Indicator Technology, will check an estimated 24 million foreigners each year, though some will be repeat visitors.** The only exceptions will be visitors from 28 countries — mostly European nations whose citizens are allowed to come to the United States for up to 90 days without visas.

Source: <http://www.cnn.com/2003/TRAVEL/12/23/airport.security.ap/ind ex.html>

10. *December 23, ABC TV7 (Denver, CO)* — **Trooper: radioactive waste almost made it through tunnel.** A Colorado State Trooper stopped a tractor-trailer Sunday, December 21, for an equipment violation and said the driver was trying to drive 40,000 pounds of low-level radioactive waste illegally through the Eisenhower Tunnel at midnight. **No trucks carrying**

hazardous material are allowed to use the tunnel, which goes under the Continental Divide. Those trucks are required, by law, to use U.S. Highway 6 over Loveland Pass. Trooper Lloyd Smith also found other violations and stopped the driver from proceeding any further. The Missouri-based shipping company was notified and the driver was issued two misdemeanor summons. Troopers plan to keep track of trucks from the shipping company to make sure its drivers comply with Colorado's hazardous materials rules.

Source: <http://www.thedenverchannel.com/news/2723255/detail.html>

11. *December 23, Sentinel & Enterprise (Fitchburg, MA)* — **Emergency management urging vigilance. Local emergency management officials worry that terrorists are targeting public transportation systems and are monitoring them closely in reaction to this week's heightened terror alert.** Charles Coggins, director of the Leominster Emergency Management team, said he is in contact with the chiefs of the police and fire departments and the public health director via e-mail to share information about vulnerable areas in the city. He said, "In Leominster we are carefully watching the North Leominster rail. It carries some hazardous materials through here." **Coggins said railroad police are not only checking cargo more frequently but also inspecting cars, passengers and the tracks themselves.** Mohammed Khan, director of the Fitchburg-based Montachusett Regional Transit Authority (MART), said MART hires private security officers to patrol the Intermodal station on lower Main Street. Khan said the Massachusetts Bay Transit Authority commuter rail that runs through Fitchburg, North Leominster, and Shirley is of most concern to his agency because it "can carry any type of material and anything can happen on the line."

Source: <http://www.sentinelandenterprise.com/Stories/0.1413.106~4994~1848661.00.html>

[\[Return to top\]](#)

Postal and Shipping Sector

12. *December 23, DM News* — **New Merlin program . The U.S. Postal Service (USPS) will begin using its Mail Evaluation Readability and Lookup Instrument, or Merlin, to validate address accuracy January 1 despite concerns from some mailers.** Merlin verifies barcode readability and other mail requirements. As of January 1 the postal service will use Merlin to read, parse, and validate addresses against barcodes for greater accuracy. Specifically, it will analyze barcode digit strings and check for what it calls "gross" address accuracy errors. The USPS said that it will allow a one percent tolerance for some address accuracy errors, but no tolerance for the incorrect use of ZIP+4 codes 0000 or 9999. "If we have add-on codes that are incorrect or pretty blatant errors, it makes us inefficient and costs us more to process the mail and to provide service to that mail piece," said John Sadler, manager, business mail acceptance, USPS. **Mailers are concerned that there will be no grace period to test the new process before the zero-tolerance rule begins.**

Source: http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=25963

13. *December 23, DM News* — **Judge rules Astar Air meets U.S. citizenship rules.** A U.S. Department of Transportation administrative law judge issued a recommended decision Friday that Astar Air Cargo, formerly DHL Airways, is owned and controlled by U.S. citizens, allowing the airline to continue hauling packages domestically and internationally for Deutsche Post's DHL Worldwide Express unit. The ruling was a setback

for FedEx Corp. and UPS Inc. Both had challenged the ownership and control structure of DHL Airways. Congress ordered the Department of Transportation (DOT) to review its previous conclusion that DHL Airways was a U.S. company and not an arm of Brussels-based DHL Worldwide Express. Under federal law, an airline owned or controlled by a foreign entity cannot carry passengers or freight within the U.S. **Since the ruling is a "recommended decision," DOT officials will review his findings. All parties will get a chance to petition the department for discretionary review with the final decision expected in 2004. It is uncommon for the agency to overrule an opinion of an administrative judge.** The losing side can appeal any final decision to the federal courts.

Source: http://www.dnnews.com/cgi-bin/artprevbot.cgi?article_id=2600_3

[\[Return to top\]](#)

Agriculture Sector

14. *December 23, USAgNet* — **China bans poultry imports from South Korea.** China banned the import of any poultry or bird products from South Korea after a bird flu virus spread beyond a quarantined zone. **In a joint statement, the Chinese Ministry of Agriculture and State Administration of Quality Supervision, Inspection and Quarantine also said all South Korean bird products must be returned or destroyed,** the Xinhua news agency reported. By Monday nine South Korean farms had been hit by the H5N1 virus, which can potentially harm humans, the country's agriculture ministry said. The ministry confirmed new outbreaks of the highly contagious disease at poultry farms more than 120 miles away from the site of the initial outbreak a week ago. Around 950,000 chickens or ducks had by Monday been slaughtered or were destined to be culled to contain the spread of disease, it said.

Source: <http://www.usagnet.com/story-national.cfm?Id=1380&yr=2003>

15. *December 23, Associated Press* — **First suspect case of mad cow in U.S. The first-ever U.S. case of mad cow disease is suspected in a single cow in Washington state, but the American food supply is safe, Agriculture Secretary Ann Veneman said Tuesday.** She told a news conference that a single Holstein cow that was either sick or injured, thus never destined for the U.S. food supply, tested presumptively positive for the brain-wasting illness. Mad cow disease, known also as bovine spongiform encephalopathy, is a disease that eats holes in the brains of cattle. It sprang up in Britain in 1986 and spread through countries in Europe and Asia, prompting massive destruction of herds and decimating the European beef industry. Veneman said the apparently diseased cow was found at a farm in Mabton, WA. She said the farm has been quarantined. **Samples from the cow have been sent to Great Britain for confirmation of the preliminary mad cow finding, she said.** Veneman said a tissue sample from the suspect U.S. cow was taken on December 9 and had been tested at a lab in Iowa.

Source: <http://www.nynewsday.com/news/ny-usmadcow1224.0.6747920.print.story?coll=nyc-topnews-short-navigation>

16. *December 22, Associated Press* — **Chicken virus smuggling. Three former executives of a Maine laboratory have been indicted in connection with a scheme to smuggle a chicken virus into the country from Saudi Arabia so they could produce a vaccine.** The case dates back to 1998, when a Maine Biological customer in Saudi Arabia discovered one of its chicken flocks had avian influenza. To produce a vaccine, Maine Biological required a sample of the

virus, which was then smuggled into the United States. After producing a vaccine, company officials are accused of falsifying production records and shipping documents to send it back to the Saudi customer. **"It posed a significant threat to poultry farms," U.S. Attorney Paula Silsby said.** Another batch of the vaccine was produced, but before it could be shipped company officials were informed somebody had tipped off the government about what it was doing, according to the indictment. The employees allegedly loaded the vaccine into a truck and disposed of it before the laboratory could be inspected by U.S. Department of Agriculture officials. Maine Biological's officers also agreed to affix labels that falsely stated the contents of vaccines for some overseas customers because the licenses for that vaccine hadn't been issued by the importing country, the indictment says.

Source: <http://news.mainetoday.com/apwire/D7VJKS8O1-355.shtml>

17. *December 22, San Francisco Chronicle* — **Olive flies infesting North Bay crops.** The olive fly, a pest that took hold in Southern California five years ago, swept with unexpected speed through Napa and Sonoma counties this fall. Hobbyists, boutique oil makers, and some commercial growers discovered the infestation too late. The olive flies, long a problem in European olive orchards but new to California, don't ruin the trees but can destroy a year's crop and damage the oil's flavor. **The number of olive flies caught in Napa County monitoring traps exploded this fall, going from 120 a week at their November 2002 peak to 1,200 a week at their peak this year.** The flies are so tiny that often they're detected only after they've wrought their havoc and olives, which serve as nurseries for the flies' larvae, start rotting or don't ripen. The olive fruit fly is here to stay. **Unlike the Mediterranean fruit fly and the grapevine-destroying sharpshooter, which the state fights to eradicate every time they pop up, the olive fly was so endemic by the time it was discovered that the decision was made to learn to live with it.** While the fly hasn't affected olive oil prices yet, growers say they'll eventually have to pass on the cost if the fly isn't controlled.

Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2003/12/22/BAG6N3SBNU1.DTL>

[\[Return to top\]](#)

Food Sector

Nothing to report.

[\[Return to top\]](#)

Water Sector

18. *December 23, Associated Press* — **Theft suspected cause of ammonia leak.** A chemical leak at a water-treatment plant near Pride, LA, could have been caused by someone trying to steal ammonia, a key ingredient in methamphetamine, police said. The leak happened Monday morning and injured at least two people and shut down roads, said Lt. Darrell O'Neal of the East Baton Rouge Parish Sheriff's Office. **"Evidently, someone cut the line and tried to siphon off some ammonia," O'Neal said.** Detectives are investigating the idea that someone wanted to steal the ammonia to make crystal meth, O'Neal said. The Baton Rouge Fire Department's Hazardous Materials team shut off the valve that was allowing the ammonia to leak, Fire Department spokesman Howard Ward said. Area residents were told to stay in their

homes, close windows, and turn off air conditioners.

Source: <http://www.nola.com/newsflash/louisiana/index.ssf?/base/news-6/1072164241204500.xml>

[[Return to top](#)]

Public Health Sector

19. *December 23, Associated Press* — **Judge halts forced military anthrax shots. Ruling that some use of the anthrax vaccine is experimental, U.S. District Judge Emmet G. Sullivan said Monday that servicemen should not have to take the vaccine unless they consent.** The government has maintained that the licensed vaccine is safe, is not experimental, and can protect against anthrax inhaled or absorbed through the skin. **In granting the preliminary injunction, Sullivan ordered the government to respond by January 30.** The government approved the vaccine three decades ago, and it is used to protect veterinarians and scientists who work with anthrax. Plaintiffs in the case, unidentified active duty, National Guard, and civilian defense employees, say the license covered only exposure through the skin. Other uses might not be safe, they contend. In his ruling, Sullivan cited a 1998 law that prohibits the use of new drugs or those unapproved for their intended use unless people being given the drug have consented to its use or the president has waived the consent requirement. The government does not recommend vaccinating the general public but says the vaccine overall is very safe, with rare severe side effects.

Source: http://www.sunspot.net/features/health/ats-ap_health12dec23.0.7524219.story?coll=sns-health-headlines

20. *December 23, European Space Agency* — **Satellites will provide Ebola clues. The European Space Agency (ESA) is set to gather satellite data to help resolve the scientific enigma of the Ebola virus.** Whenever Ebola strikes Central Africa it can kill in large numbers. **Ebola's natural host organism or reservoir remains unknown. "Humans get infected only when an individual gets into contact with an already-infected animal,"** said Ghislain Moussavou of the Gabon-based International Center for Medical Research (CIRMF). Starting next year ESA will be supplying Earth Observation data of the region to CIRMF as one component of a new project called Epidemio. Characterizing the ecological parameters of the whole area of study can't be done by ground-based means. By mapping the areas where infected animals are found, areas with similar environmental features can be highlighted as suspected sites for priority study. And in future CIRMF plans to begin a study of Ebola antibody prevalence in the human population, helping to identify potential infection risk zones. **Detailed meteorological data could be important because the periodicity of Ebola outbreaks points to a seasonal component: "This suggests particular ecological conditions could characterize the reservoir host habitat,"** Moussavou concluded.

Source: <http://www.sciencedaily.com/releases/2003/12/031223062412.htm>

21. *December 23, Food and Drug Administration* — **FDA investigating reports of unlicensed influenza vaccine.** The Food and Drug Administration (FDA) has received reports of potential distribution of unlicensed influenza vaccine in the United States. The Agency is aggressively working with State health authorities and the Centers for Disease Control and Prevention (CDC) to investigate the source and quality of influenza vaccine being made available through

unusual suppliers. **Specifically, FDA has received reports of offers to sell unlicensed influenza vaccine in the U.S., and of individuals who are not licensed health care professionals administering questionable influenza vaccine in apparent efforts to take advantage of reports that influenza vaccine is in short supply.** FDA is actively investigating these reports and taking prompt action, when appropriate. For example, FDA and the Florida Department of Health worked together to prevent unlicensed product from entering the country and being offered for sale.

Source: <http://www.fda.gov/bbs/topics/ANSWERS/2003/ANS01275.html>

22. *December 22, Scripps Howard News Service* — **Hospitals pass on new germs.** Exchanges of antibiotic-resistant germs between patients in intensive-care units is "unexpectedly high," according to a new study. **Researchers from the Karolinska Institute in Sweden found that 70 percent of intensive-care patients they studied were colonized with bacteria from other patients in the unit.** The team, led by Charlotta Edlund, took swabs in intensive-care units from the upper and lower airways of 20 patients who had required mechanical assistance in breathing for least three days. They focused on transmission of several strains of staphylococcus bacteria. "These species have the ability to survive in the ICU surroundings on medical devices and equipment for weeks to months," Edlund said. The researchers cultured bacteria from the swabs and analyzed genetic fingerprints of the various strains to tell which were identical or closely related, and thus assess the transmission rate between patients. **Seventeen of the patients were colonized by the staph strains during their hospital stay. In six of them, the bacteria had reached the lower airways after the patient was ventilated, suggesting that the procedure itself had introduced the bacteria. Fourteen of the patients had either passed on a bacterial strain to another patient or received a bacterial strain from another patient.**

Source: http://www.courierpress.com/ecp/health/article/0,1626,ECP_75_6_2522903,00.html

[\[Return to top\]](#)

Government Sector

23. *December 23, CNN* — **Pentagon to conduct terror drill.** The Pentagon Tuesday morning is scheduled to conduct a so-called "continuity-of-government" exercise, scheduled as a direct result of the heightened terror threat level, U.S. officials said. **During the exercise, key Pentagon officials are to be notified that they are to move immediately to secret locations where the government has established alternative facilities, according to the officials.** The exercise involves only high-level Pentagon officials, although Defense Secretary Donald Rumsfeld is not expected to participate, officials said. The drill is designed to protect Pentagon authorities in the event of an attack. Missile batteries were being moved into place around Washington, and possibly around New York City, and "irregular air patrols" were ordered because of what one senior Pentagon official called "specific, reliable, credible" intelligence regarding a possible terror strike.

Source: <http://www.cnn.com/2003/US/12/23/threat.level/index.html>

[\[Return to top\]](#)

Emergency Services Sector

24. *December 23, Government Executive Magazine* — **Agencies respond to increased terrorist threat level.** Federal agencies put action plans into effect Monday in response to an increased national threat level, but some officials said heightened security requirements create budget and personnel burdens for their agencies. **Such plans vary by agency. For example, the Transportation Security Administration implemented five new security steps at the nation's airports. The FBI ordered its 56 field offices to keep their command centers open 24 hours a day. The Federal Air Marshal Service increased the number of armed guards flying on domestic flights. The Pentagon increased air patrols and deployed anti-aircraft batteries around Washington, and the Coast Guard increased the number of air and sea patrols.** Federal officials said their agencies were meeting the heightened security requirements, but some cited budget and personnel concerns. For example, the National Park Service spent \$2 million on overtime pay and per diem allowances when the national threat level was raised in September 2002, said spokesman David Barna. Most of that cost came from temporarily reassigning park rangers in the western United States to places that might be targets of attack, such as the Washington Monument.

Source: <http://www.govexec.com/dailyfed/1203/122203c1.htm>

[[Return to top](#)]

Information and Telecommunications Sector

25. *December 22, Federal Computer Week* — **NIST releases security level guidance.** The National Institute of Standards and Technology (NIST) released a draft of the last piece of guidance for agencies to determine the proper level of security on information systems last week. The "Special Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories" provides the middle step for guidance and standards required under the Federal Information Security Management Act (FISMA) of 2002. **NIST's categories of security impact are based on draft Federal Information Processing Standard (FIPS) 199, which the division released in September. The goal of the guidance is to have agencies assign impact levels without considering potential security controls and countermeasures, but in October, NIST released another draft guide outlining minimum-security controls for each category.** NIST also released a draft interagency report on smart card technology development and adoption within agencies. The draft report is in response to a January General Accounting Office report that recommended that NIST play a greater role in smart card implementation governmentwide. Additional information is available on the NIST Website: <http://csrc.nist.gov/publications/drafts.html>
Source: <http://fcw.com/fcw/articles/2003/1222/web-nist-12-22-03.asp>

26. *December 22, CNET News.com* — **Apple issues patch for Mac OS X hole.** Apple Computer has issued a security update that, among other fixes, closes a hole in Mac OS X that could have allowed hackers to take control of a computer under particular circumstances. **The patch essentially changes the default settings for connecting to a Dynamic Host Communication Protocol (DHCP) server on Mac OS X 10.2.8. (aka "Jaguar"), Mac OS X 10.3.2 (aka "Panther") and the corresponding server versions of these operating systems. A DHCP**

server assigns a TCP/IP address to a computer and, under the earlier default settings, a Mac running one of the above-listed OSes would accept data from DHCP servers found on a local area network. If a hacker inserted a malicious DHCP server on a local network, he or she could then exploit Apple's earlier default setting to embed malicious software on a computer or use the computer as a drone for coordinated attacks on other systems. **Apple's security update also fixes a buffer overflow vulnerability in a file system, plugs another vulnerability in Panther that could cause denial-of-service requests** and in general improves the security features of the affected OSes. Additional information available on Apple's Website:

<http://docs.info.apple.com/article.html?artnum=61798>

Source: http://news.com.com/2100-7355_3-5130853.html?tag=nefd_top

27. *December 22, eWEEK* — **MySQL Quashes Defects in Database Release. MySQL AB on Monday, December 22, released Version 4.0.17 of its MySQL open-source database software. The update features a number of cleaned up code defects.** Available in source code and binary form, the MySQL 4.0.17 maintenance release for the current MySQL production version corrects all valid bugs discovered during an October poll conducted within the development community via an independent study. According to the study, **21 software defects in 235,667 lines of MySQL source code were found.** The report's Defect Summary noted 15 defect instances of NULL Pointer Deference, three defect instances of an allocated memory leak, and three defect instances of an uninitialized variable prior to usage. Additional information is available on the MySQL Website:

<http://www.mysql.com/downloads/mysql-4.0.html>

Source: <http://www.eweek.com/article2/0.4149.1420119.00.asp>

28. *December 22, eSecurity Planet* — **Sober mutant starts to squirm.** Anti-virus vendors on Monday, December 22, issued upgraded threat warnings for a mutant of the W32/Sober-C worm now squirming its way through e-mail in-boxes. **The mass-mailer, which also spreads via file-sharing on P2P networks, has added a bilingual element and arrives with a range of attachment filenames--EXE, SCR, PIF, COM, CMD or BAT.** Chris Beltoff of Sophos Inc. said the **increased sightings of a mass-mailing virus at the height of the Christmas shopping season puts new PC owners at the highest risk.** "The risk is high because of the new, unprotected computers that are being sold off the shelf. Depending on how long that PC has been sitting on the shelf, it's likely new PCs are unprotected against the latest viruses. Remember, the average consumer isn't going to make patching his main priority on a new computer, Beltoff said. Network Associates warned that 80 percent of the intercepted virus comes from Germany and said the characteristics of Sober-C has put Germans or users in German-speaking regions at higher risk.

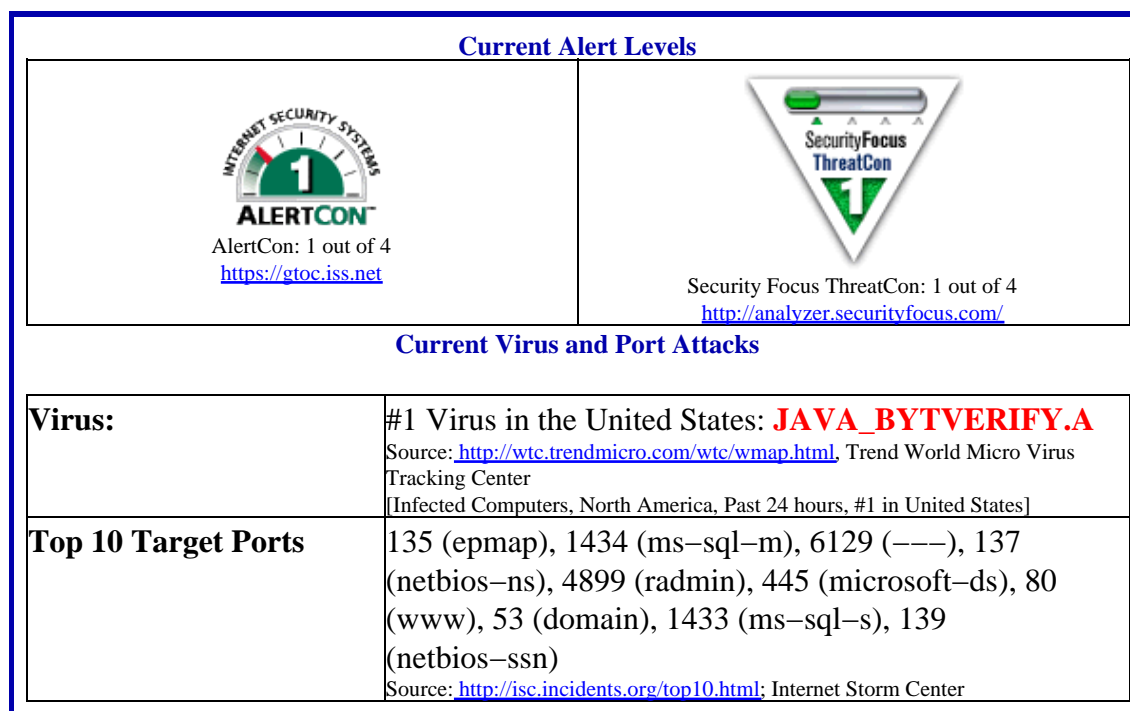
Source: <http://www.esecurityplanet.com/trends/article.php/3291951>

29. *December 22, Federal Communications Commission* — **FCC releases data on high-speed services for Internet access.** The Federal Communications Commission (FCC) Monday, December 22, released summary statistics of its latest data on the deployment of high-speed connections to the Internet in the United States. **Facilities-based service providers file data with the FCC on the amount of high-speed connections in service twice a year pursuant to the FCC's local competition and broadband data gathering program (FCC Form 477).** The FCC adopted the local competition and broadband data gathering program in March 2000 to assist the FCC in its efforts to monitor and further implement the pro-competitive,

deregulatory provisions of the Telecommunications Act of 1996. **The FCC uses data from this effort to evaluate the deployment of advanced telecommunications capability.** The statistics summarize FCC Form 477 filings due from qualifying providers on September 1, and reflect data as of June 30. They also include state-by-state, population density, and household income information, ranked by zip codes.

Source: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-242398_A1.pdf

Internet Alert Dashboard



[\[Return to top\]](#)

General Sector

30. *December 23, Reuters* — Arms experts may have helped Iran, Pakistan says. Pakistan admitted on Tuesday that scientists involved in its nuclear weapons program might have been driven by "personal ambition or greed" to export technology to Iran, but added the government had no part in any such deals. The Foreign Ministry spokesman, Masood Khan, said Pakistan was determined to get to the bottom of allegations that nuclear technology may have been transferred to Iran. He said the government began questioning scientists from a state-run laboratory five to six weeks ago after approaches by the International Atomic Energy Agency and information from the Iranian government. On Monday, December 22, Islamabad revealed that Abdul Qadeer Khan, revered as a national hero for developing a nuclear bomb tested in 1998 to match that of its rival India, was being questioned in connection with "debriefings" of several scientists working at his Khan Research Laboratories, a uranium enrichment plant near Islamabad.

Source: <http://www.iht.com/articles/122589.htm>

31. *December 23, Firehouse.com* — **Pipe bomb found at Ohio gas station. A Columbus, OH, gas station was closed for several hours Monday after a pipe bomb was discovered in a nearby alley.** The device was found in an alley near a Marathon station, located at 1680 S. High St., NewsChannel 4's Beth Dal Ponte reported. **Police said that the report might not have been an isolated incident.** "At 6:38 a.m., we received a call from a citizen that found what he thought was a pipe bomb in the alley behind the gas station," said Columbus police Sgt. Mike Robinson. The bomb squad was called to the scene and local homeowners were told to stay inside their homes, Dal Ponte reported. "They came out and detonated the device and found that it, in fact, was a pipe bomb," Robinson said. "Right in the time frame that it happened, that is our busiest time right there," said Kimberly Hammond, a Marathon employee. "A lot of people came back and wanted to know what's going on." **Robinson said a battalion chief advised him that they had another run at a nearby car lot several days ago when a pipe bomb was found.** A few blocks east of the scene, at Woodrow and Parsons avenues, officers said that they heard a small explosion during roll call but did not find anything. Investigators said that they would follow up on several leads in hopes of getting more information.
Source: http://cms.firehouse.com/content/article/article.jsp?section_Id=46&id=23576

32. *December 23, Associated Press* — **Turkish cops charge suspect with aiding bombers, find fertilizer in home.** Mehmet Kus was arrested after police allegedly found enough chemical fertilizer in his home to fill five truck bombs like those used in the Istanbul suicide bombings last month, news reports said. **An arrested relative of Habip Aktas, a suspected leader of al Qaeda in Turkey, helped lead police to the 12 large sacks of chemical fertilizer at Kus's home in Istanbul,** the Vatan and Sabah newspapers reported. Private NTV television carried a similar report. Cables and explosives were also seized in the raid at the house, Sabah reported. The fertilizer was the same as that used to make the bombs in the four attacks, according to Vatan and Sabah. On Tuesday, a State Security Court in Istanbul that deals with terrorism cases charged Kus with aiding and abetting terrorists, the semiofficial Anatolia news agency reported. Conviction on those charges carries a maximum penalty of five years in prison. More than 30 people have been charged so far in connection with the attacks last month that killed 62 people. Al Qaeda involvement is suspected in the bombings, which targeted two synagogues, a London-based bank and the British Consulate. **Police also detained a suspected top member of al Qaeda in Turkey, the semi-official Anatolia news agency reported.** The agency said Harun Ilhan was detained in the central city of Konya.
Source: http://www.canoe.ca/CNEWS/World/WarOnTerrorism/2003/12/23/29_5682-ap.html

[[Return to top](#)]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipic.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Warnings](#) – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on

material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Publications](#) – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703–883–6631

Subscription and Distribution Information Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703–883–6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202–323–3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open–source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.